Confiance numérique ou autonomie, il faut choisir

Par Jean-Paul SMETS
Fondateur de l'éditeur de logiciels libres Nexedi

Le numérique de confiance, le rôle exorbitant de l'Agence nationale de sécurité des systèmes d'information et l'inflation réglementaire européenne créent des conditions de marché défavorables aux nombreuses technologies européennes du numérique et aux logiciels libres. Ils accélèrent ensemble l'adoption en France de technologies américaines de *cloud* non immunes à des accès non autorisés par un État tiers. Ils augmentent le risque de panne générale en favorisant des offres de *cloud* centralisées peu résilientes. En matière de gestion du risque cyber, la notion de « transparence » offre une alternative à la « confiance » pour renforcer l'autonomie industrielle européenne dans le numérique sur une base technologique résiliente et immune à un accès non autorisé par un État tiers.

Lancée le 17 mai 2021 par Bruno Le Maire, la Stratégie nationale du *cloud*[1] introduit « le *cloud* de confiance » avec pour objectifs « la protection maximale des données (…), l'accès aux meilleurs services mondiaux (...) et la cohérence avec les initiatives européennes » comme Gaia-X. Elle postule que « les meilleures entreprises de services mondiaux (...) sont américaines. » et annonce que « Microsoft ou Google, pourraient licencier tout ou partie de leur technologie à des entreprises françaises ». Deux ans après cette annonce, nos données hébergées sur des *clouds* américains ne sont pas protégées, que ce soit chez les grands opérateurs de santé comme Doctolib[2] qui subit des fuites de données sensibles ou avec le *Health Data Hub*[3] qui poursuit son activité en violation du Règlement général pour la protection des données (RGPD)[4]. Des technologies de *cloud* de Google et de Microsoft ont été acquises sous licence par des entreprises françaises mais ne sont toujours pas commercialisées[5]. L'adoption des services américains de *cloud* s'est accélérée[6] et notre dépendance technologique accrue. L'accès des technologies européennes de *cloud* aux marchés publics français a été entravé. L'innovation européenne dans le *cloud* a parfois été freinée. Le logiciel libre européen a été discriminé. Et l'on charge désormais un comité stratégique de filière d'appliquer la notion de « confiance numérique » à l'intelligence arti-

[1] LE MAIRE B. (2021), « Déclaration de M. Bruno Le Maire, ministre de l'économie, des finances et de la relance, sur la stratégie nationale du *cloud* », mai, Paris, France.

[2] JONNIAUX A. (2023), « Doctolib perd des milliers de données médicales sensibles », *Journal du Geek*, 5 mai.

[3] VITARD A. (2022), « Microsoft restera l'hébergeur du *Health Data Hub* jusqu'en 2025 », *L'usine digitale*, 13 septembre.

[4] CNIL (2020), « Le Conseil d'État demande au *Health Data Hub* des garanties supplémentaires pour limiter le risque de transfert vers les États-Unis », octobre, Paris, France.

[5] THALES (2022), « Thales présente S3NS en partenariat avec Google *cloud* et dévoile son offre de transition vers le *cloud* de confiance », juin, Paris, France.

[6] FOUILLAND F. & GALAS G. (2022), « Souveraineté numérique – La guerre du *cloud* doit avoir lieu », Soutenance finale à l'école des mines de Paris, juin, Paris, France.

ficielle, au logiciel, aux technologies immersives et au quantique[7] avec comme probable résultat une perte d'autonomie généralisée si les effets de la « confiance » y sont les mêmes que dans le *cloud*.

Nous allons illustrer sur le cas du *cloud* les mécanismes qui conduisent une politique publique de « confiance numérique » à engendrer une perte d'autonomie. Nous proposerons ensuite la notion de « transparence » comme une alternative à la « confiance » dépourvue de ses effets délétères sur l'autonomie.

Le *cloud* « made in USA » privilégié au nom de la confiance

L'Europe a créé plus de 300 technologies de *cloud* qui ont fait leurs preuves avec plus de 1 200 références ou études de cas identifiées par le fonds de dotation du libre[8]. On y trouve des technologies d'infrastructure (IaaS), des technologies pour accélérer le travail des équipes de développement de logiciels (PaaS) et des services destinés aux utilisateurs finaux (SaaS). Environ 15 % des entreprises à l'origine de ces technologies ont pour clients de grands opérateurs de *cloud* américains qui en ont équipé leur infrastructure. Ainsi, le service de base de données sur le *cloud* d'Amazon Web Services (AWS) s'appuie sur la base de données suédo-finlandaise MariaDB et sur le logiciel autrichien de stockage hautes performances Linbit[9]. On trouve dans cette liste de nombreux autres fournisseurs européens de technologies d'infrastructure de *cloud*, matériel comme logiciel.

Le 31 mai 2023, la Première ministre annonçait une actualisation de la doctrine d'utilisation du *cloud* par l'État visant à préciser la notion de données sensibles[10]. Il est ainsi rappelé l'obligation, depuis une précédente circulaire du 5 juillet 2021 en matière d'achat public de *cloud* commercial, d'assurer « l'hébergement des données d'une sensibilité particulière par des solutions disposant de la qualification SecNumCloud délivrée par l'Agence nationale de sécurité des systèmes d'information ». La nouvelle circulaire précise les conditions d'application en exigeant de la solution retenue qu'elle soit « immunisée au droit extracommunautaire » et « immunisée contre tout accès non autorisé par des autorités publiques d'État tiers ».

Elle définit par ailleurs les données sensibles comme celles « dont la violation est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé et la vie des personnes ou à la protection de la propriété intellectuelle » ainsi que celles comportant des « secrets protégés par la loi, notamment au titre des articles L.311-5 et L.311-6 ». Cette définition comprenant à la fois « le secret de la vie privée » et le « le secret des affaires », son champ d'application est potentiellement large et peut inciter les services de l'État à considérer toutes leurs données comme sensibles, comme lors d'un appel d'offres

[7] POLLET M. (2022), « Numérique de confiance : les premiers pas du nouveau comité stratégique de filière », *L'usine digitale*, 22 novembre.

[8] FRANCK S. (2022), "Cloudrepo.eu – A directory of European cloud technologies [vidéo]", Euclidia NOW! Towards a resilient cloud infrastructure in Europe, 29 septembre, Bruxelles, Belgique, repéré à https://www.euclidia.eu/news/euclidia-Website.Euclidia.Now.Brussels

[9] FRANCK S. (2022), "Linbit: high performance storage architecture [vidéo]", Euclidia NOW! Towards a resilient cloud infrastructure in Europe, 29 septembre, Bruxelles, Belgique, repéré à https://www.euclidia.eu/news/euclidia-Website.Euclidia.Now.Brussels

[10] BORNE E. (2023), « Actualisation de la doctrine d'utilisation de l'informatique en nuage par l'État (*cloud* au centre) », 31 mai, Paris, France.

pour l'hébergement des sites Web d'information du gouvernement ouvert uniquement aux solutions qualifiées « SecNumCloud »[11].

Pour les projets existants, la circulaire précise qu'une « dérogation (…) pourra être accordée (…) sans qu'elle ne puisse aller au-delà de douze mois après la date à laquelle une offre de *cloud* acceptable (…) sera disponible en France. ». En l'absence d'offre jugée « acceptable », ce qui ne signifie pas qu'il n'existe pas de solutions fonctionnelles, la dérogation est de durée indéfinie comme pour le *Health Data Hub*[12].

Nous avons donc consulté, sur le site de l'Agence nationale de sécurité des systèmes d'information, la liste des solutions d'infrastructure (IaaS) qualifiées « SecNumCloud » au 20 juillet 2023[13]. On y trouve trois offres fondées sur un cœur logiciel d'infrastructure VMWare (Atos, Cloud Temple, OVH) et une offre fondée sur un cœur logiciel d'infrastructure CISCO Unified Computing System (Outscale). La quatrième offre (Oodrive) ne concerne pas l'infrastructure (IaaS).

	Date de début de la qualification	Date de fin de la qualification	Niveau de recommandation	IaaS	PaaS	SaaS	Référence de la qualification
Informatique en nuage (SecNumCloud)							
Cloud Temple							
Secure Temple	15/03/2022	15/03/2025	✓	×			569
Oodrive							
Oodrive platform avec le service Oodrive_meet	09/05/2023	22/01/2025	✓			×	766
Oodrive platform avec le service Oodrive_work	09/05/2023	22/01/2025	✓			×	768
Oodrive platform avec le service Oodrive_work_share	09/05/2023	22/01/2025	✓			×	770
Outscale SAS							
IaaS Cloud on Demand	09/06/2023	30/11/2023	✓	×			958
OVH							
Private Cloud	05/06/2023	23/12/2023	✓	×			937
Worldline							
Worldline Cloud Services - Secured IaaS	22/10/2021	22/10/2024	✓	×			2686

Figure 1 : Offres d'informatique en nuages qualifiées « SecNumCloud » au 20 juillet 2023.

Or, comme l'a révélé Edouard Snowden[14], des portes dérobées sont systématiquement introduites dans les logiciels et matériels conçus aux États-Unis. C'est aussi probablement le cas des matériels et logiciels produits en Chine ou en Europe.

VMWare et CISCO UCS étant des logiciels d'origine américaine fournis sous forme binaire et sans accès au code source, il est difficile d'en supprimer les portes dérobées éventuelles. On peut donc conclure qu'aucune offre commerciale ne répond aux exigences simultanées

[11] SPM (2021), « Appel d'offres pour l'hébergement internet des sites des services du Premier ministre », 22 septembre, Paris, France.

[12] LATOMBE P. (2023), « Communiqué de presse : Le *Health Data Hub* refuse d'engager sa migration *cloud* vers une solution souveraine européenne avant le T3 de 2025 (...) », 3 mai, Assemblée nationale, Paris, France.

[13] ANSSI (2023), « Liste des produits et services qualifiés », 20 juillet, Paris, France.

[14] SNYDER B. (2014), "Snowden: The NSA planted backdoors in Cisco products", *Infoworld*, 15 mai.

de qualification « SecNumCloud » et d'immunité « contre tout accès non autorisé par des autorités publiques d'État tiers ». Seule une offre déconnectée de tout réseau public pourrait éventuellement répondre à ces deux critères.

Quant aux *clouds* internes de l'État « Nubo » et « Pi », ils s'appuient tous deux sur le logiciel libre « OpenStack » édité par une fondation de droit américain, dont 85 % des sponsors « platine » sont américains ou chinois[15]. Ce sont les seules offres de *cloud* éventuellement conformes aux deux critères de qualification et d'immunité. Le logiciel « OpenStack » a depuis été abandonné par une grande partie de ses intégrateurs[16] en raison de difficultés techniques : on peut s'interroger sur sa viabilité notamment en termes de cybersécurité. À moins de déconnecter ces *clouds* d'Internet, l'usage de processeurs Intel ou AMD sur les *clouds* internes de l'État ne permet pas non plus de garantir l'immunité « contre tout accès non autorisé par des autorités publiques d'État tiers » en raison de l'intégration à ces processeurs de dispositifs techniques de prise de contrôle à distance[17].

Il existe pourtant de nombreuses offres européennes de logiciel d'infrastructure (OpenNebula, OpenSVC, Proxmox, Nexedi, Vates, Virtuozzo, etc.) et de microprocesseur (Kalray, NXP, ST, etc.). Plusieurs opérateurs de *cloud*, dont Scaleway, ont proposé de fournir le code source et les plans de leur infrastructure de *cloud* pour que l'État en opère une copie sous son contrôle.

Toutes ces informations étaient connues de l'État avant 2021[18]. L'État a néanmoins choisi une stratégie conduisant dans les faits à exclure des marchés publics les offres de *cloud* d'origine technologique européenne et à favoriser des offres d'origine technologique américaine. Cette stratégie creuse la balance extérieure, détruit les compétences européennes dans les PME du numérique et ne garantit ni l'absence de portes dérobées ni l'immunité de nos infrastructures.

L'ANSSI, frein à la résilience

Le mécanisme clef de l'exclusion des marchés publics des offres technologiques européennes est la qualification « SecNumCloud »[19] délivrée par l'Agence nationale de sécurité des systèmes d'information (ANSSI). Il prolonge un préjugé exprimé devant l'Assemblée nationale par son directeur à l'époque : « le développement logiciel n'est pas le point fort de la France et ne l'a jamais été »[20]. Ce préjugé peut s'expliquer par les nombreux échecs de grandes entreprises françaises dans le domaine du logiciel : défaillances du système d'écoutes de la justice[21], échec du projet de *cloud* souverain Cloudwatt[22], fiches de paie loufoques dans l'armée[23], etc.

---

[15] OPENINFRA FOUNDATION (2022), "2022 Annual Report", Austin, Texas, USA.

[16] VAUGHAN-NICOLS S. (2019), "SUSE drops OpenStack Cloud", *ZDNet*, 9 octobre.

[17] CLABURN T. (2017), "Intel Management Engine pwned by buffer overflow", *The Register*, 6 décembre.

[18] FDL (2020), « Gaia-X : un *cloud* européen sans les industriels européens du *cloud* ? », 25 août, La Madeleine, France.

[19] ANSSI (2022), « Prestataires de services d'informatique en nuage (SecNumCloud) – référentiel d'exigences », version 3.2, 8 mars, Paris, France.

[20] BRIDEY J.-J. (2018), « Audition de M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information, sur le projet de loi de programmation militaire », Assemblée nationale, 8 mars, Paris, France.

[21] DUMOULIN S. (2016), « Thalès embarrassé par la panne de son système d'écoutes judiciaires », *Les Échos*, 14 mars.

[22] DEBES F. (2019), « Une page se tourne pour le *cloud* souverain français », *Les Échos*, 1er août.

[23] RELTIEN P. (2018), « Louvois, le logiciel qui a mis l'armée à terre », *France Inter*, 27 janvier.

Ces mêmes entreprises, pourtant à l'origine de nombreux échecs, n'ont pas eu de difficulté à obtenir la qualification « SecNumCloud » auprès de l'ANSSI. Ce que privilégie cette qualification, c'est avant tout la centralisation des infrastructures et la formalisation des procédures : centralisation de la gestion des risques, procédures d'agrément des fournisseurs, procédure de vérification d'antécédents des candidats à l'embauche, procédure de contrôle d'accès aux installations physiques, etc. Les grandes entreprises françaises du numérique excellent dans ce domaine, tout comme leurs consœurs à l'international.

Ce préjugé de l'ANSSI s'explique aussi par l'omission du tissu de PME européennes extrêmement compétitives dans le domaine du logiciel et dont les principaux clients sont à l'export. La société grenobloise VATES, éditeur du logiciel d'infrastructure XCP-NG, propose un équivalent français de VMWare, le logiciel propriétaire américain utilisé dans la quasi-totalité des *clouds* qualifiés « SecNumCloud » à ce jour. VATES réalise 95 % de son chiffre d'affaires à l'export. Le projet scikit-learn, hébergé par la fondation INRIA, est le *leader* des outils d'apprentissage, l'une des branches les plus utilisées de l'intelligence artificielle. Il a parmi ses financeurs Microsoft, Fujitsu et le Boston Consulting Group.

Ensemble, les PME européennes sont capables de proposer des offres de *cloud* compétitives, pionnières et complètes, du IaaS au PaaS en passant par le *edge computing* industriel et la 5G virtualisée[24]. Leur organisation sous forme de réseau de petits fournisseurs indépendants les uns des autres permet en outre de se prémunir contre une « panne générale », phénomène observé régulièrement sur les grands réseaux de télécommunication malgré toutes les précautions prises par les opérateurs[25] ou sur le *cloud* de Google dont l'incendie[26] parisien en mai 2023 a perturbé l'ensemble des services dans le monde. Lorsqu'une infrastructure s'appuie sur plusieurs opérateurs de centres d'hébergement gérés selon des procédures distinctes, sur plusieurs fournisseurs de transit Internet indépendants, sur des logiciels d'infrastructure et sur des services applicatifs aux fonctions similaires mais d'origines diverses, il est rare que l'ensemble des services tombe en panne au même moment. Au lieu de pannes géantes mais peu fréquentes, une approche répartie multi-fournisseurs conduit à des pannes plus fréquentes mais limitées et sans interruption de service grâce à la redondance entre fournisseurs.

C'est ce que l'on appelle la résilience[27].

Mais la qualification « SecNumCloud » est d'autant plus coûteuse qu'elle nécessite d'agréer un grand nombre de sous-traitants indépendants. Cela favorise des offres monolithiques gérées par une seule grande entreprise – moins résilientes – au détriment des offres issues d'un district industriel de PME – plus résilientes.

La doctrine de l'ANSSI tend par ailleurs à promouvoir une gestion centralisée du risque au travers d'outils de surveillance appelés « boîtes noires » qu'il est plus simple et moins coûteux de placer en un seul point de passage de l'information plutôt qu'en des milliers de points de passage. Les « boîtes noires » ont été légalisées en 2015 par la loi sur le renseignement[28], étendues en 2021 par une nouvelle loi sur le renseignement[29] et renforcées en 2023 par la loi de programmation militaire sous le nom de « sondes » de recueil de

[24] EUCLIDIA (2021), "Strategic autonomy now", p. 10, Luxembourg Internet Days, Luxembourg.

[25] LEROY T. (2023), « Orange : une panne nationale empêche de passer des appels sur mobiles », *BFM Tech & Co*, 30 mai.

[26] SHARWOOD S. (2023), "Google Cloud's watery Parisian outage enters third week, with no end in sight", *The Register*, 10 mai.

[27] FERMIGIER S. (2013), « Groupe thématique logiciel libre. Contribution au plan industriel *cloud* », p. 7, Systematic Paris Region, 20 décembre.

[28] REES M. (2015), « Surveillance et boîte noire au menu de la loi sur le renseignement », Nextinpact, 18 mars.

[29] ADAM L. (2021), « Loi renseignement 2 : Le retour des boîtes noires », *ZDNet*, 28 avril.

données[30]. C'est une même agence qui est donc en charge de déployer des outils d'atteinte à la vie privée ou au secret des affaires, et d'instruire une qualification de services de *cloud* visant à protéger la vie privée et le secret des affaires.

Les conflits de missions auxquels l'ANSSI fait face ont pu la conduire à freiner des projets de recherche dans le domaine de la résilience et des architectures réparties, bien que ce ne soit pas son rôle. Le projet de recherche « SimpleRAN » lancé dans le cadre de la stratégie d'accélération 5G de l'État a par exemple subi un retard d'un an à cause de l'ANSSI qui souhaitait que son architecture résiliente soit modifiée pour fonctionner de façon centralisée et qu'elle puisse accueillir des boîtes noires, ce qui revenait à vider une partie du projet de son sens. Ce n'est qu'après avoir accepté formellement ces exigences que le projet a été approuvé. Les membres du projet ont en réalité pris la décision d'abandonner le marché français de la résilience et de ne rien faire qui conduise à violer la vie privée ou le secret des affaires ; il existe par ailleurs suffisamment de besoins de résilience à l'export alors que les pannes de grandes infrastructures ne cessent de croître[31] et que le Splinternet menace la continuité d'Internet[32].

Loin de se cantonner aux marchés publics d'État ou à un rôle de censeur de la politique industrielle, les pouvoirs exorbitants de l'ANSSI seront étendus avec la directive NIS2[33] qui lui confèrent « la possibilité d'émettre des instructions contraignantes » et d'agir comme une « police répressive à l'encontre des entreprises, de plus en plus guidées et ralenties par des contraintes législatives et réglementaires », accélérant ainsi la concentration du marché français autour des technologies de quelques multinationales américaines au détriment de notre résilience.

Le logiciel libre européen discriminé

Les logiciels libres, en associant de nombreux développeurs à la création d'une œuvre partagée, sont une des formes les plus abouties de district industriel[34]. Les logiciels libres sont créés et édités en Europe principalement par des PME et par des auteurs individuels, plus rarement par des organismes à but non lucratif. Leur sécurité s'appuie sur des mécanismes sociaux de confiance partagée fondés sur la reconnaissance mutuelle entre pairs et non sur des procédures bureaucratiques d'audit.

Les mécanismes sociaux de confiance partagée sont proscrits par la qualification « SecNumCloud » qui oblige les utilisateurs de logiciels libres à vérifier ligne à ligne chaque contribution au code de chaque logiciel libre utilisé dans le cadre d'un processus d'audit formel. Ce n'est pas le cas avec un logiciel propriétaire d'infrastructure (par exemple VMWare) pour lequel un contrat peut suffire à condition qu'il comprenne les clauses requises par l'ANSSI. Ce n'est pas le cas non plus avec un logiciel propriétaire d'infrastructure « à base de logiciel libre » issu d'un grand éditeur américain (par exemple IBM) et doté d'un contrat similaire.

Une PME européenne éditrice de logiciel libre n'est hélas pas en mesure de proposer ce type de contrat en raison des risques et des lourdeurs qu'il ferait peser sur elle et qu'elle ne pourra pas financer. La création européenne de logiciels libres, souvent remarquable

[30] ALOMAR B. (2023), « La loi de programmation militaire risque de percuter la doctrine du "*cloud* de confiance" », *Le Monde*, 24 mai.

[31] SMETS J.-P. (2023), "Cloud outages are on the rise. Here's why", *Fortune*, 7 juin.

[32] KRIM T. (2023), "Is the Breakup of the Internet inevitable?", DLD, Munich, Allemagne, 12 janvier.

[33] PETIOT L. (2022), « Directive NIS2 : les enjeux de la nouvelle cybersécurité européenne », *Contrepoints*, 4 décembre.

[34] TWOWINGS *et al.* (2009), « District industriel », Wikipedia.

et majoritairement issue de PMEs, se retrouve ainsi discriminée par rapport aux logiciels propriétaires issus de grands éditeurs, majoritairement américains.

Ce n'est pas la première attaque récente contre les solutions libres européennes.

En 2021, la direction générale des Entreprises[35] lançait un processus de rapprochement européen en vue de constituer des projets importants d'intérêt européen commun (PIIEC) dotés de larges subventions. Cependant, elle favorisait les grands intégrateurs français et omettait de nombreux fournisseurs européens de logiciels d'infrastructure de *cloud*. Les projets finalement validés, portés par des intégrateurs partenaires de Google, favorisaient les logiciels libres de Google plutôt que ceux d'éditeurs européens de logiciels libres équivalents. Une note d'étonnement dénonçant une entente a été transmise par plusieurs éditeurs européens aux autorités nationales et européennes en charge de la concurrence.

Le 24 janvier 2023, la direction interministérielle du Numérique (DINUM) organisait une réunion de promotion de solutions propriétaires de *cloud* pour les équipes de développement[36]. Il existe pourtant une offre européenne compétitive de *cloud* libre dont la promotion auprès des administrations fait explicitement partie des missions de la DINUM conformément à la loi du 7 octobre 2016 pour une République numérique[37].

Le 15 septembre 2022, la Commission européenne posait avec le « Cyber Resilience Act »[38] un principe de responsabilité des ayants droit pour toute faille de sécurité présente dans un logiciel libre. L'ayant droit d'un logiciel libre s'expose ainsi à une amende de 15 millions d'euros dans le cas où son logiciel, intégré à un produit commercialisé par un tiers, serait à l'origine d'un incident de cybersécurité, et ce quand bien même il n'aurait jamais été rémunéré pour cela. Seule échappatoire pour l'ayant droit : céder son actif logiciel à une fondation de logiciel libre, le plus souvent américaine. Pour les autres, la Commission européenne estime dans son étude d'impact que cette régulation impliquera un minimum de 25 000 € de frais administratifs par logiciel et une augmentation de 30 % des coûts de développement[39], un niveau bien trop élevé pour favoriser la croissance de l'écosystème des éditeurs de logiciels libres dont la Commission reconnaît pourtant la nécessité pour atteindre l'indépendance numérique[40].

La proposition publiée le 28 septembre 2022 pour réviser la directive sur la responsabilité du fait des produits défectueux instaure un régime de responsabilité stricte qui pourrait accroître encore plus le risque pour les ayants droit de logiciels libres[41]. Tout comme dans le « Cyber Resilience Act », la notion d'usage non commercial d'un logiciel libre[42] n'exonère pas les ayants droit d'éventuelles poursuites pour des usages de leur logiciel quand bien même ils n'auraient pas été rémunérés.

[35] O C. (2021), « PIIEC *cloud* : Lancement du processus de rapprochement européen », 6 octobre, Ljubljana, Slovénie.

[36] DINUM (2023), « L'État dans le nuage : une journée dédiée au *cloud* », 24 janvier, Paris, France.

[37] LEMAIRE A. (2016), « Loi n°2016-1321 du 7 octobre 2016 pour une République numérique », *Journal Officiel*, 7 octobre.

[38] EUROPEAN COMMISSION (2022), "Cyber Resilience Act", 15 septembre, Bruxelles, Belgique.

[39] EUROPEAN COMMISSION (2022), "Impact Assessment Report", 15 septembre, Bruxelles, Belgique.

[40] EUROPEAN COMMISSION (2020), "Open source software strategy 2020-2023", 21 octobre, Bruxelles, Belgique.

[41] BUSINESSEUROPE *et al.* (2023), "Proposed Product Liability Directive revision may undermine Europe's competitiveness", 15 mai.

[42] DE LUCA S. (2023), "New Product Liability Directive", European Parliamentary Research Service, Mai, Bruxelles, Belgique.

La proposition de règlement du 15 mai 2023 sur l'intelligence artificielle[43] propose de subordonner le droit de publier un logiciel – libre ou non – à la vérification d'une dizaine de critères allant du respect de la démocratie à la réduction des émissions de gaz à effet serre en passant par la vérification de l'adéquation de toute nouvelle ligne de code produite à l'ensemble des lois de l'Union européenne au moyen d'un système de gestion de la traçabilité. Ces exigences, qui impliquent un surcoût important pour un logiciel propriétaire sont fondamentalement incompatibles avec le processus de développement des logiciels libres. Avec un logiciel libre, on commence par publier son code avant de collaborer. Avec le règlement, on commence par faire un audit avant de pouvoir collaborer, ce qui freine la collaboration au point de la rendre impraticable.

Quant à la révision de mai 2023 de la doctrine « *cloud* au centre », elle restreint l'obligation d'usage de logiciels libres aux seuls « communs numériques contributifs », une définition qui exclut les éditeurs européens de logiciels libres contrairement à la notion de « bien public numérique » qui, elle, inclut le secteur privé[44]. La notion retenue de « commun numérique » offre ainsi aux services de l'État une base légale pour développer des logiciels concurrents de logiciels libres déjà disponibles au prétexte qu'un logiciel libre d'éditeur européen ne serait pas un commun et que l'on ne pourrait donc pas lui faire confiance.

La transparence, alternative à la confiance pour préserver l'autonomie

La politique « *cloud* de confiance » et la norme « SecNumCloud » ont été imaginées par certains comme un outil de protectionnisme déguisé sous une norme technique et donc compatible avec le traité de l'Organisation mondiale du commerce (OMC). En pratique, son effet a été l'inverse du protectionnisme. La « confiance » a multiplié les barrières à l'entrée pour les fournisseurs européens de technologies de *cloud* et a accéléré l'adoption de technologies américaines de *cloud* peu sûres. Il eut été plus simple d'appuyer une politique protectionniste sur des bases légales déjà éprouvées telles que l'exception culturelle, le Règlement général pour la protection des données (RGPD) ou des obligations fortes de réversibilité déjà présentes dans le code des marchés publics[45].

L'impératif de la cybersécurité pourrait néanmoins expliquer la poursuite en France d'une politique de numérique de confiance malgré des effets délétères désormais évidents en matière d'autonomie. L'accroissement des tensions internationales a fait de la cybersécurité une priorité absolue, y compris au détriment de notre résilience. L'État achète ses technologies de *cloud* aux États-Unis plutôt qu'en Europe pour les mêmes raisons que nos voisins européens achètent leurs avions de combat aux États-Unis plutôt qu'en Europe[46] : cela répond à un besoin de protection et d'assistance ; charge ensuite à des intégrateurs nationaux d'en assurer la distribution et l'entretien.

Nous ne sous-estimons pas ici l'importance des enjeux liés à la cybersécurité. Tous les systèmes informatiques que nous utilisons comportent un nombre de failles incommensurable que même les plus grandes entreprises dotées de processus formels d'audit rigoureux

[43] BENIFEI B. & TUDORACHE I.-D. (2023), "Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts", Draft compromise amendments, European Parliament, 16 mai.

[44] NORAD, UNDP & UNICEF (2023), "Promoting digital public goods to create a more equitable world".

[45] SMETS J.-P. (2022), « Qu'est-ce qu'un *cloud* libre ? », *Les Annales des Mines - Enjeux numériques*, juin.

[46] SPINELLI F., SMETS J.-P. & LECHELLE Y. (2021), « Défense, *cloud* souverain : les PME au centre de notre indépendance », *Les Échos*, 12 juillet.

ne parviennent pas à contenir[47]. Ces failles existent car la charge cognitive nécessaire pour mesurer l'impact cyber d'une ligne de code écrite dans un langage de programmation de conception ancienne tel que « C » est supérieure à la capacité du cerveau humain. En l'absence d'une nouvelle génération de systèmes d'exploitation et de langages de programmation intégrant la cybersécurité dans leurs principes de conception, éliminer les failles de cybersécurité revient à boucher les trous d'un tamis dont la surface grandirait plus vite que les zones déjà bouchées.

Plutôt que de faire croire aux clients du *cloud* qu'une qualification les protégera de tout risque, comme par magie, il serait plus honnête et conforme au devoir de conseil de leur décrire en toute transparence l'absence relative de cybersécurité. Cela leur permettra d'organiser leur défense en ayant conscience de la réalité des risques.

Peut-on garantir en France qu'un processeur Intel ne comporte pas de portes dérobées destinées à un État tiers ? non ; qu'un processeur ST ne comporte pas de portes dérobées destinées à un État tiers ? oui, à condition qu'il ait été audité par des autorités françaises compétentes et produit en France ; que le code de Linux ne comporte pas de failles permettant un accès à distance à un État tiers ? non ; qu'un code écrit en python n'accédera pas aux données d'un autre processus sans en avoir les permissions ? non, mais cela arrivera moins souvent qu'avec un code écrit en C grâce à la protection mémoire partielle offerte par l'interpréteur.

Ces faits étant acceptés par le client, une discussion peut alors s'engager sur la base d'une grille d'analyse de risque partagée en toute transparence avec le fournisseur. Où sont stockés les mots de passe et les clés de chiffrement pour accéder aux bases de données ? Peut-on dédier un serveur physique à un seul client ? La police peut-elle demander une copie du disque dur du serveur ? Quel est le délai moyen entre l'annonce publique d'une vulnérabilité et sa prise en compte dans une mise à jour ? Quels moyens sont proposés au client pour vérifier la véracité des réponses fournies ? Les autres questions de cette grille sont le résultat d'un effort collaboratif entre clients et fournisseurs.

Les réponses à cette grille d'analyse permettent ensuite au client de décider contre quels risques il souhaite se protéger et comment il souhaite se protéger. On a remplacé la notion binaire de « confiance » par une notion de « transparence » à plusieurs dimensions.

Chaque client, chaque application ayant des besoins et des priorités différents en matière de risque, une grille d'analyse permet de comparer les offres en fonction des réels besoins plutôt qu'en sélectionnant l'offre dite de « confiance », c'est-à-dire l'offre qui cocherait tous les besoins de cybersécurité de toutes les applications de tous les clients… et n'existe pas. On ouvre ainsi le marché à une grande diversité de fournisseurs, certains – souvent européens – disposant de meilleurs services dans le domaine de la résilience ou du temps réel et d'autres – souvent américains – disposant d'interfaces utilisateur intuitives moins génératrices d'erreurs par les utilisateurs ou permettant de se connecter au bouclier cyber du commandement américain

Alors que la confiance produit de l'obscurité sur le marché, la transparence fluidifie le marché en évitant les phénomènes de concentration, d'entente ou de barrières non douanières. Alors que la confiance favorise les technologies américaines, la transparence accélère l'adoption des fournisseurs européens de technologies numériques dont le succès à l'export reste la meilleure démonstration de leurs avantages compétitifs et dont l'existence est indispensable à notre autonomie.

[47] ARGHIRE I. (2023), "Severe Azure vulnerability led to unauthenticated remote code execution", SecurityWeek, 31 mars.